




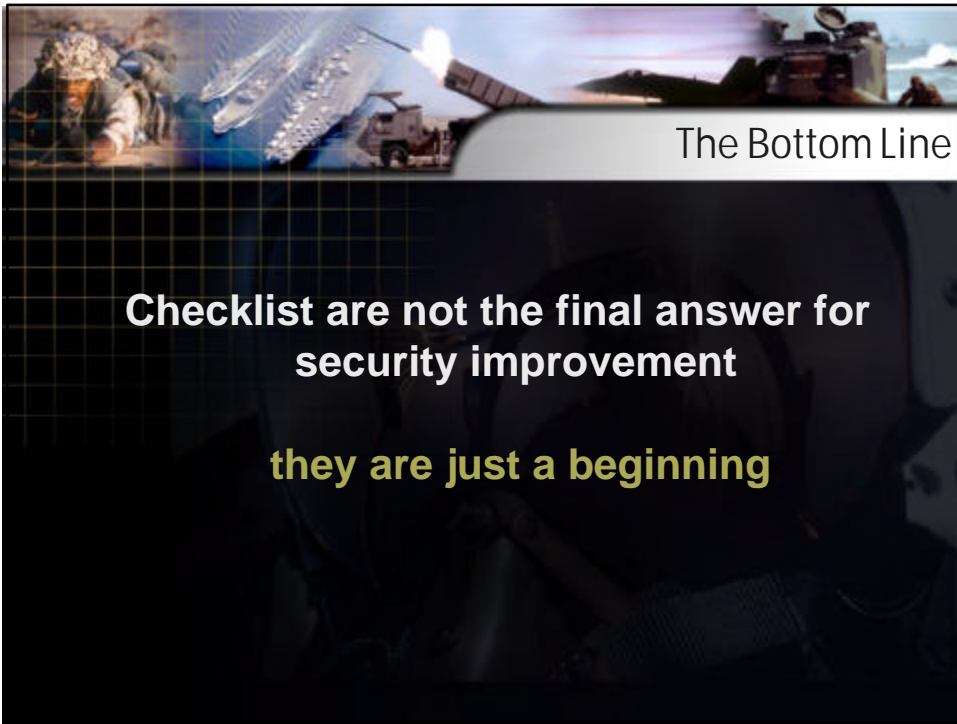
Deployment and Verification of Checklists

Paul Bartock
NSA



Importance of Consensus Security Benchmarks

- **A Shared Problem**
Connected networks are dependent upon the security of the other
- **Consensus is nice, Security improvement is better**
Security guidance is only valuable when used and when it become part of designing, installing and operating our networks
- **Provides real Security “Value”**
Example: Consensus Security Benchmarks for Windows 2000 , conservatively close well over 80% of the known vulnerabilities



The Bottom Line


**Checklist are not the final answer for
security improvement**

they are just a beginning



Real Security Improvement
Will Come

- **When system owners and decision makers move to adopt consensus for Operational networks**
- **When Consensus Security Benchmarks are supported by tools to help manage networks**
- **When Consensus Security Benchmarks are available for each of the key components found in our networks**
- **When the Consensus Security Benchmarks are supported with training**
- **When we change our security decision processes**



Benefits

- **Safer system procurement (by providing specifications)**
- **Appliance vulnerability reduction (by engaging the manufacturers)**
- **Leverage community partnership**
- **Vendor Supported Security Configurations**
- **Security Evaluation tools based on implemented Benchmarks can score, measure and report compliance**



Where We Are Today

- **Consensus Windows 2000 Baseline Security Settings**
 - *Richard Clarke - July 17, 2002 – “model for gov’t / industry cooperation”*
- **DISA FSO’s Security Technical Implementation Guidance**
- **Center for Internet Security**
 - *Benchmarks for Solaris, HP-UX, Linux, and Windows NT, 2000.*
 - *Tools to check configuration and guide administrator in application of benchmark*
- **Industry**
 - *Bindview – tools to check configuration and apply benchmark.*
 - *Microsoft – developed configuration guidance*



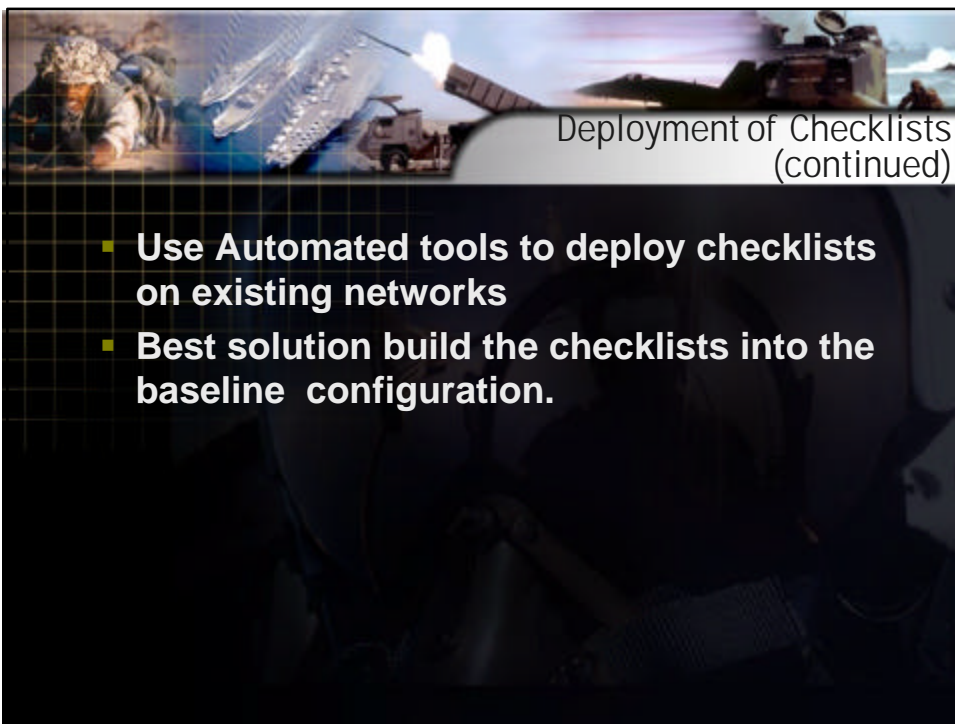
Trends

- **Industry acceptance**
 - *Dell: selling W2K workstations configured to CIS Benchmark*
 - *Cisco will configure routers to benchmark*
 - *MS and Mitre senior engineers report using benchmarks.*
- **Gov't acceptance**
 - *Air Force CIO – W2K consensus benchmark an AF standard*
 - *Intell Community draft policy that mandates use of NSA configuration guides for SCI IS.*



Deployment of Checklists

- **System Administrators and Management agrees on the checklists as the security standard for the network**
- **System Architecture and design start from the benchmark / checklists**
- **Security engineers tailor the checklists based on program specific security issues and operational constraints**
- **Documentation of security-operational tradeoffs and serves as evidence to decision makers about security worthiness of the resulting system**



Deployment of Checklists (continued)

- **Use Automated tools to deploy checklists on existing networks**
- **Best solution build the checklists into the baseline configuration.**



Verification of Checklists

- **Use security evaluation tools which supports periodic or continuous reporting on actual setting of every machine in the network.**

